Deutscher Bundestag **Drucksache 18/10182**

18. Wahlperiode 02.11.2016

Gesetzentwurf

des Bundesrates

Entwurf eines ... Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch

A. Problem und Ziel

In letzter Zeit häufen sich die Angriffe auf Internetseiten mittels sogenannter „Distributed-denial-of-service (DDos)“-Attacken, bei denen eine Vielzahl von in krimineller Absicht ausgelösten Anfragen, die an Webseiten gerichtet werden, dazu führen, dass diese vorübergehend unerreichbar sind. Zudem finden gezielte Cyberangriffe auf mit dem Internet verbundene Kritische Infrastrukturen, also Einrichtungen wie große Industrieanlagen, Elektrizitätswerke, Staudämme, Anlagen der Wasserversorgung oder Telekommunikationsanlagen, statt, die diese beschädigen, empfindlich stören oder unbrauchbar machen sollen. Die bekanntesten Fälle in jüngster Zeit waren die Internet-Angriffe auf den Deutschen Bundestag in 2015, auf ein deutsches Stahlwerk in 2014, bei dem ein Hochofen beschädigt wurde, sowie die Attacken auf den französischen Sender TV5 und die belgische Zeitung Le Soir in 2015. Die letzten beiden Begebenheiten zeigen, dass sich auch Terroristen dieses Mittels bedienen.

Jüngst wurde erstmals eine Schadsoftware in einem deutschen Atomkraftwerk entdeckt[1].

Das massenhafte Auftreten von sogenannten „Erpressungs-Trojanern“ oder „Krypto-Trojanern“ – allein bei einer Variante wurden über 5 000 Neuinfektionen in Deutschland pro Stunde festgestellt[2] – verursacht große Schäden, auch die öffentliche Verwaltung und Kritische Infrastrukturen sind betroffen.[3]

Die Werkzeuge, mit denen Straftäter diese Handlungen begehen, sind regelmäßig sogenannte „Botnetze“. Als ein Botnetz bezeichnet man eine große Anzahl von mit dem Internet ständig oder zeitweise verbundener informationstechnischer Systeme wie Computer oder Mobiltelefone, die – von ihrem rechtmäßigen Nutzer

---

1 Vgl. http://www.spiegel.de/netzwelt/web/grundremmingen-computervirus-im-atomkraftwerk-entdeckt-a-1089248.html

2 Vgl. http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

3 Vgl. http://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html
http://www.t-online.de/computer/sicherheit/id_76362038/teslacrypt-erpresser-trojaner-legt-deutsche-behoerden-lahm.html

unbemerkt – mit Schadprogrammen infiltriert sind und daher einzeln oder in ihrer Gesamtheit einer fremden Kontrolle unterliegen. Große Botnetze umfassen mehrere Millionen Opferrechner, die von dem jeweiligen sie kontrollierenden Täter einzeln oder zusammen ferngesteuert werden können. Botnetze sind auch Handelswaren, die über kriminelle Märkte im Internet in Gänze oder in Teilen verkauft, verliehen oder vermietet werden.

Die Infiltration der Opfersysteme geschieht auf unterschiedliche Weise. Neben dem Anklicken von Links in Spam-E-Mails oder dem Öffnen infizierter Dateianhänge kann eine Infektion etwa auch dadurch erfolgen, dass der rechtmäßige Nutzer mit seinem informationstechnischen System eine legitime Internetseite aufsucht, die zuvor von den Tätern unerkannt präpariert wurde (sogenannte „drive-by infection“). Die Täter schleusen dabei einen Schadcode in die Webseite ein, der dazu führt, dass auf dem Opfersystem im Hintergrund heimlich Schadprogramme aufgespielt werden und er so zum „Bot“ (von englischen „robot“) wird, also zu einem durch Dritte unerkannt fernsteuerbaren Zombie-Computer, dessen sämtliche Funktionen und Daten nunmehr eben jenem Dritten, der ihn infiziert hat, offenstehen.

Gegen diese Art der Infektion kann sich auch der aufmerksame Computernutzer kaum zur Wehr setzen. Zurzeit geht man davon aus, dass bis zu 40 Prozent aller internetfähigen informationstechnischen Systeme in Deutschland mit Schadsoftware verseucht sind und damit potentielle Bots darstellen.

Die Gefahren von Botnetzen liegen aber nicht nur in ihrem möglichen Einsatz zur Durchführung von DDos-Attacken. Sie stellen gleichzeitig eine der wichtigsten Täterinfrastrukturen im Bereich der Cyberkriminalität dar. Sie werden genutzt zum Versenden von Spam-Emails, zur Begehung von Betrug im Onlinebanking oder zur Verschleierung des Standortes von Servern mit kriminellen Inhalten.

Ferner können die infiltrierten Opfersysteme als Anonymisierungswerkzeuge verwendet werden. Die Täter können mit ihrer Hilfe unerkannt Internetdienste nutzen und kommunizieren. Durch diese Art der Verwendung erlangen infiltrierte Opfersysteme eine erhebliche Bedeutung für Kriminelle auch außerhalb des Phänomenbereichs Cybercrime.

Darüber hinaus ist die Kontrolle über die Bots durch den Täter, also die infizierten Opfersysteme, vollständig, d. h. sämtliche auf der Festplatte gespeicherten oder im Arbeitsspeicher befindlichen Daten des legitimen Benutzers stehen den Tätern offen; sie können diese beliebig ausspähen oder kopieren. Gleiches gilt für Daten, die der Nutzer extern, etwa bei Clouddiensten, gespeichert hat, denn die Täter können ihren Zugriff auch auf alle mit dem infiltrierten System verbundenen Systeme ausdehnen.

In strafrechtlicher Hinsicht eröffnet die umfassende Vernetzung unterschiedlicher IT-Systeme wie etwa Produktionsanlagen, Marketing, Vertrieb und Einkauf, die gemeinhin mit dem Begriff „Industrie 4.0“ bezeichnet wird, neue Angriffsflächen für kriminelle Aktivitäten in einem bisher nie dagewesenen Ausmaß. Es werden IT-Systeme angreifbar, die bislang aus dem Internet nicht erreichbar waren. Dadurch vergrößert sich das Risiko existenzgefährdender Situationen durch Ausfall oder Fehlfunktion von Produktions- oder Geschäftsprozessen erheblich.

Welches Ausmaß die heimliche Infiltration der Bürger durch international agierende Straftäter hat, wurde im Jahre 2014 offenbar, als im Rahmen von Botnetzermittlungen über 14 Millionen ausgespähte Datensätze aufgefunden wurden.

Weiterhin kann der gesamte Internetverkehr der Opfer durch die Straftäter abgehört und manipuliert werden. Auch die Computerhardware des Opfersystems kann unbeschränkt ferngesteuert werden, so können z. B. Webcam oder Mikrofon

unbemerkt eingeschaltet werden, um aus den Räumen der Opfer heimlich Videos und Töne zu übertragen. Damit wird der heimische Laptop oder das Mobiltelefon zu einem machtvollen Ausspähwerkzeug in den Händen international agierender Cyberkrimineller.

Hierdurch ist die Integrität und Vertraulichkeit des infiltrierten informationstechnischen Systems vollständig aufgehoben, ohne dass der legitime Benutzer es bemerkt. Weitreichende Rückschlüsse auf seine Persönlichkeit bis in den Kernbereich höchstpersönlicher Lebensgestaltung sind möglich. Heutige Smartphones spiegeln häufig nahezu die gesamten privaten und z. T. auch die geschäftlichen oder beruflichen Aktivitäten ihrer Benutzer wider. Die Bedeutung mobiler IT-Systeme wird weiter wachsen, sie dienen zunehmend als Mittel zur Bezahlung von Waren und Dienstleistungen. Schon jetzt wird prognostiziert, dass mobile IT-Systeme Zahlungskarten in diesem Bereich in ihrer Bedeutung überholen werden.

Es ist gegenwärtig kaum absehbar, welche Anwendungen in der Zukunft noch möglich werden.

Das Bundesverfassungsgericht hat bereits 2007 in seiner wegweisenden Entscheidung zum Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes, vgl. 1 BvR 370/07, 1 BvR 595/07) die bestehenden Gefahren für die Bürger dargestellt. Zutreffend hat das Bundesverfassungsgericht zudem festgestellt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist. Die Relevanz der Informationstechnik für die Lebensgestaltung des Einzelnen erschöpft sich nicht in der größeren Verbreitung und Leistungsfähigkeit von Personalcomputern. Daneben enthalten zahlreiche Gegenstände, mit denen große Teile der Bevölkerung alltäglich umgehen, informationstechnische Komponenten. So liegt es beispielsweise zunehmend bei Telekommunikationsgeräten oder elektronischen Geräten, die in Wohnungen oder Kraftfahrzeugen enthalten sind (BVerfG a. a. O.). Weiter führt das BVerfG aus:

„Der Einzelne kann […] Zugriffe zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Informationstechnische Systeme haben mittlerweile einen derart hohen Komplexitätsgrad erreicht, dass ein wirkungsvoller sozialer oder technischer Selbstschutz erhebliche Schwierigkeiten aufwerfen und zumindest den durchschnittlichen Nutzer überfordern kann. Ein technischer Selbstschutz kann zudem mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sein. Viele Selbstschutzmöglichkeiten – etwa die Verschlüsselung oder die Verschleierung sensibler Daten – werden überdies weitgehend wirkungslos, wenn Dritten die Infiltration des Systems, auf dem die Daten abgelegt worden sind, einmal gelungen ist. Schließlich kann angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen."

Es ist daher die Aufgabe auch des Strafrechts, den lückenlosen Schutz des bedeutsamen Grundrechts auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sicherzustellen.

Der strafrechtliche Schutz der Integrität und Vertraulichkeit von informationstechnischen Systemen wird im Kernstrafrecht derzeit im Wesentlichen durch die §§ 202a, 303a und 303b StGB gewährt.

Dieser Schutz ist indes lückenhaft.

So betrifft § 202a StGB nur das Ausspähen solcher Daten, die durch eine besondere Zugangssicherung geschützt sind. Zudem greift diese Norm nur dann ein,

wenn der Täter unter Überwindung der Zugangssicherung handelt. Das bedeutet, dass derzeit die Frage, ob der strafrechtliche Schutz eines informationstechnischen Systems gegeben ist oder nicht, allein auf den Schultern der Opfer ruht.

Aber selbst wenn eine Zugangssicherung aktiviert ist, sind die Schutzlücken erheblich.

Fallbeispiel:

Das Opfer befindet sich im öffentlichen Raum, z. B. in einem Zug. Um zu telefonieren, gibt es den PIN-Code zur Entsperrung seines Smartphones ein. Der Täter beobachtet das und merkt sich die PIN. Anschließend, nachdem das Opfer sein Smartphone wieder eingesteckt hat, gelingt es dem Täter, das Gerät – vom Opfer unbemerkt – an sich zu bringen und es mittels des PIN-Codes zu entsperren, um anschließend private oder auch geschäftliche Daten auszulesen oder Fotos zu betrachten. Danach steckt der Täter das Smartphone zurück in die Tasche des Opfers.

Die mit der Hand eingegebene PIN ist kein taugliches Tatobjekt i. S. v. § 202a Absatz 2 StGB, so dass das Beobachten der Eingabe nicht strafbar ist. Der anschließende Einsatz der beobachteten Zahlenkombination durch den Täter hebt bestimmungsgemäß den entsprechenden Zugangsschutz auf, so dass es am „Überwinden“ der Zugangssicherung fehlt. Eine Überwindung i. S. v. § 202a Absatz 1 StGB soll nämlich dann nicht gegeben sein, wenn nur noch ein unerheblicher technischer oder zeitlicher Aufwand erforderlich ist[4].

Ergebnis: Der Täter ist im Kernstrafrecht gegenwärtig straflos[5].

Auch in den Fällen, in denen Täter unabhängig voneinander vorgehen, also ohne dass die Voraussetzungen des § 25 Absatz 2, der §§ 26 oder 27 StGB vorliegen, ist die Straflosigkeit der Datenausspähung nach § 202a StGB gegeben. Dies ist z. B. dann gegeben, wenn ein allein handelnder Täter massenhaft Opfersysteme infiziert, um den Zugriff auf die infiltrierten Systeme anschließend über anonyme Internet-Handelsplattformen an ihm nicht bekannte Personen zu verkaufen. Kauft ein Dritter den Zugriff auf ein infiltriertes informationstechnisches System an und späht sodann die dort gespeicherten Daten aus, handelt er nicht unter Überwindung einer Zugangssicherung und ist nicht gemäß § 202a StGB bestrafbar[6].

Die zunehmende Steigerung der Effektivität von Schadprogrammen und das Auftreten von sogenannter „fileless malware“, also Schadsoftware, die keine Veränderungen an gespeicherten Daten herbeiführt[7], führen dazu, dass auch der Schutz durch § 303a StGB lückenhaft ist. Die Strafbarkeit nach dieser Norm setzt voraus, dass der Täter auf dem betroffenen informationstechnischen System gespeicherte Daten im Sinne von § 202a StGB löscht, verändert etc. Die Infiltration informationstechnischer Systeme ist heutzutage jedoch auch ohne die Veränderung von gespeicherten Daten möglich. Neben dem Einsatz von „fileless malware“ kann dies z. B. durch sogenannten Hardwaretrojaner[8] geschehen.

---

[4] Vgl. Hilgendorf in: Leipziger Komm. zum StGB, 12. Aufl. 2010 , § 202a Rn. 36 (str.).

[5] Str., vgl. Graf NStZ 2007, 129, 131, der auch für den Fall des als das Hinterlassen des Passwortes am Arbeitsplatz für den Administrator, der nach Dienstschluss den Rechner für den Arbeitnehmer an dessen Bedürfnisse anpassen will, und welches nun stattdessen der hierzu nicht befugte Kollege auffindet, es liest und dann auch benutzt zum gleichen Ergebnis gelangt.

[6] Vgl. Roos/Schumacher MMR 2014, 377, 380 f.

[7] Vgl. http://www.mcafee.com/us/resources/solution-briefs/sb-quarterly-threats-nov-2015-1.pdf; http://blog.trendmicro.com/trendlabs-security-intelligence/without-a-trace-fileless-malware-spotted-in-the-wild/

[8] Vgl. http://www.heise.de/newsticker/meldung/32C3-Hardware-Trojaner-als-unterschaetzte-Gefahr-3056452.html

§ 303b StGB ist in seiner derzeitigen Fassung ebenfalls nicht geeignet, informationstechnische Systeme und insbesondere das Internet der Dinge wirksam vor Cyberangriffen zu schützen. Die Norm greift z. B. nicht bei internetgekoppelten Haushaltsgeräten oder bei ausschließlich privat genutzten Systemen, welche den überwiegenden Teil der angegriffenen Systeme darstellen.

Zwar fällt die Durchführung von DDoS-Attacken unter den Tatbestand des § 303b StGB, jedoch wird jeder sonstige Eingriff, der nicht mit einer Störung der Datenverarbeitung einhergeht, nicht erfasst.

Abgesehen von den Schutzlücken auf der Ebene der objektiven Tatbestände wird die Lückenhaftigkeit des strafrechtlichen Schutzes der genannten Normen dadurch vertieft, dass ihr Vorliegen unter den heute gegebenen technischen Rahmenbedingungen regelmäßig nicht nachweisbar ist. Häufig löschen sich Schadprogramme nach ihrem Einsatz oder bei ihrer Entdeckung selbsttätig[9], so dass selbst bei einer computerforensischen Auswertung des betroffenen informationstechnischen Systems im Nachhinein ein Tatnachweis nicht zu führen ist.

B. Lösung

Zur Erreichung eines angemessenen Schutzniveaus für die Vertraulichkeit und Integrität informationstechnischer Systeme sollen die Rechtsgedanken des § 123 StGB und des § 248b StGB in die digitale Welt übertragen und ein neuer § 202e StGB geschaffen werden. Mit der neuen Vorschrift soll die unbefugte Benutzung informationstechnischer Systeme unter Strafe gestellt werden. IT-Systeme sind mindestens ebenso schutzwürdig wie das Hausrecht und wie das ausschließliche Benutzungsrecht an Fahrzeugen. Derzeit sind sogar Fahrräder besser geschützt als Computer mit höchstpersönlichen Daten. Die Gefahr für die Allgemeinheit, die von unbefugt genutzten informationstechnischen Systemen ausgeht, ist, wie oben dargelegt, hoch.

Damit kann ein lückenloser strafrechtlicher Schutz aller Systeme und die Strafbarkeit nahezu aller Angriffsarten sichergestellt werden, denn die Infiltration von Computern und Cyberangriffe jeder Art beinhalten als Teilkomponente regelmäßig die Fernsteuerung, also das Beeinflussen oder Auslösen von informationstechnischen Vorgängen durch Dritte.

Die Formulierung des § 202e StGB-E ist technikoffen, was zu einer guten praktischen Handhabbarkeit führen und Beweis- und Abgrenzungsschwierigkeiten vermeiden soll. Technische Zufälle in der Konfiguration der Opfersysteme sollen zukünftig keine Rolle mehr spielen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

---

[9] Vgl. http://www.heise.de/security/meldung/Rombertik-Der-Virus-der-verbrannten-Erde-2633009.html

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht oder entfällt kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht oder entfällt kein Erfüllungsaufwand.

Davon Bürokratiekosten aus Informationspflichten:

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Aufgrund der Ausdehnung des deutschen Strafrechts ist zu erwarten, dass die Anzahl der Strafverfahren in einem begrenzten Ausmaß zunimmt. Dies kann zu nicht näher quantifizierbaren Haushaltsmehrausgaben bei den für die Durchführung von Strafverfahren primär zuständigen Strafverfolgungsbehörden der Länder führen. Im Zuständigkeitsbereich des Bundes anfallende Haushaltsmehrausgaben sind allenfalls in geringem Umfang zu erwarten.

Der Mehraufwand bei den Strafverfolgungs- und Vollstreckungsbehörden ist jedoch angesichts der bestehenden Strafbarkeitslücken gerechtfertigt. Zudem würden, soweit durch die – mit der Regelung ermöglichte – konsequente Strafverfolgung eine abschreckende Wirkung erreicht wird, Kosten sowie Folgekosten aus Schäden durch Cyberangriffe eingespart.

F. Weitere Kosten

Den Bürgerinnen und Bürgern sowie der Wirtschaft entstehen keine sonstigen Kosten. Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind nicht zu erwarten.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 2. November 2016

An den
Präsidenten des
Deutschen Bundestages
Herrn Prof. Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich gemäß Artikel 76 Absatz 3 des Grundgesetzes den vom Bundesrat in seiner 948. Sitzung am 23. September 2016 beschlossenen

> Entwurf eines ... Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium der Justiz und für Verbraucherschutz.

Die Auffassung der Bundesregierung zu dem Gesetzentwurf ist in der als Anlage 2 beigefügten Stellungnahme dargelegt.

Mit freundlichen Grüßen

Dr. Angela Merkel

Anlage 1

Entwurf eines ... Strafrechtsänderungsgesetzes – Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Digitaler Hausfriedensbruch

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Strafgesetzbuches

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch … geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 202d folgende Angabe eingefügt:

   „§ 202e Unbefugte Benutzung informationstechnischer Systeme“

2. Nach § 202d wird folgender § 202e eingefügt:

„§ 202e

Unbefugte Benutzung informationstechnischer Systeme

(1) Wer unbefugt

1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft,
2. ein informationstechnisches System in Gebrauch nimmt oder
3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt,

wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.

(2) Mit Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren wird bestraft, wer eine in Absatz 1 bezeichnete Handlung

1. gegen Entgelt oder
2. in der Absicht, sich oder einen Dritten zu bereichern oder einen Dritten zu schädigen,

begeht, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Straftaten unter Nutzung von informationstechnischen Systemen verbunden hat,
2. den Zugang zu einer großen Anzahl von informationstechnischen Systemen verschafft oder eine große Anzahl von informationstechnischen Systemen in Gebrauch nimmt oder eine große Anzahl von Datenverarbeitungsvorgängen oder informationstechnischen Abläufen beeinflusst oder in Gang setzt oder

3. in der Absicht handelt,

   a) eine Gefahr für die öffentliche Sicherheit,

   b) eine gemeingefährliche Straftat oder

   c) eine besonders schwere Straftat gegen die Umwelt nach § 330 herbeizuführen oder zu ermöglichen.

(4) Handelt der Täter in der Absicht, einen Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken, so ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren.

(5) Der Versuch ist strafbar.

(6) Im Sinne dieser Vorschrift ist

1. informationstechnisches System

   nur ein solches, das

   a) zur Verarbeitung personenbezogener Daten geeignet oder bestimmt ist oder

   b) Teil einer Einrichtung oder Anlage ist, die wirtschaftlichen, öffentlichen, wissenschaftlichen, künstlerischen, gemeinnützigen oder sportlichen Zwecken dient oder die den Bereichen Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Versorgung, Haustechnik oder Haushaltstechnik angehört;

2. kritische Infrastruktur

   eine Einrichtung, Anlage oder Teile davon, die

   a) den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung oder Finanz- und Versicherungswesen angehören und

   b) von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung ein erheblicher Versorgungsengpass oder eine Gefährdung für die öffentliche Sicherheit eintreten würde.

(7) Ist in den Fällen des Absatzes 1 und 2 ein Angehöriger, der Vormund oder der Betreuer verletzt oder lebt der Verletzte mit dem Täter in häuslicher Gemeinschaft, so wird die Tat nur auf Antrag verfolgt."

3. In § 205 Absatz 1 Satz 2 wird die Angabe „202b und 202d" durch die Wörter „202b, 202d und 202e Absatz 1 und 2" ersetzt.

Artikel 2

Änderung der Strafprozessordnung

Nach § 374 Absatz 1 Nummer 3 der Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch … geändert worden ist, wird folgende Nummer 3a eingefügt:

„3a. eine unbefugte Benutzung informationstechnischer Systeme (§ 202e Absatz 1 und 2 des Strafgesetzbuches),"

Artikel 3

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Die immer stärkere Verbreitung und Nutzung von Informations- und Kommunikationstechnologien, insbesondere die Nutzung des Internets, wirken sich unmittelbar auf alle Bereiche der Gesellschaft aus. Die Einbeziehung von Telekommunikations- und Informationssystemen, die eine entfernungsunabhängige Speicherung und Übertragung von Daten aller Art gestatten, bietet ein breites Spektrum neuer Möglichkeiten, aber auch des Missbrauchs.

Mit dem Einundvierzigsten Strafrechtsänderungsgesetz zur Bekämpfung der Computerkriminalität (41. StrÄndG) vom 7. August 2007 (BGBl. I S. 1786), mit welchem der deutsche Gesetzgeber dem aus dem Übereinkommen des Europarates über Computerkriminalität vom 23. November 2001 (Cybercrime Convention) sowie dem aus dem Rahmenbeschluss 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme resultierenden Umsetzungsbedarf nachgekommen ist, und mit der Einführung des Straftatbestandes der Datenhehlerei durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 wurden zuletzt Regelungen getroffen, um den Missbrauch der Informationstechnologie zu bekämpfen.

Diese genügen jedoch nicht, da die strafrechtliche Praxis gezeigt hat, dass die fortschreitende technische Entwicklung weiterhin zu spürbaren Strafbarkeitslücken führt.

Das Bundesverfassungsgericht hat in seinem Urteil zur Online-Durchsuchung vom 27. Februar 2008 als besondere Ausprägung des allgemeinen Persönlichkeitsrechts (Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 des Grundgesetzes) das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ postuliert. Damit ist dem Regelungsanliegen, IT-Systeme vor dem unbefugten Zugriff Dritter zu schützen, grundrechtliche Relevanz beizumessen (vgl. BVerfGE 120, 274 ff.).

Durch das Phänomen der schadsoftwaregestützten Existenz großer – teilweise weltumspannender – Botnetze wird dieses Grundrecht massenhaft verletzt.

Derzeit können im Kernstrafrecht zur Bekämpfung der Botnetzkriminalität vor allem die §§ 202a, 303a und 303b StGB herangezogen werden.

Diese Normen zielen indes nicht unmittelbar auf den Schutz der Vertraulichkeit und Integrität von informationstechnischer Systemen ab. § 202a StGB und § 303a StGB schützen lediglich Daten, nicht aber das technische System. § 303b StGB bezweckt zwar grundsätzlich den Schutz von Systemen. Für einen wirksamen Rechtsgüterschutz genügt es jedoch nicht, lediglich auf das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit von Daten oder auf das Interesse der Betreiber und Nutzer am störungsfreien Funktionieren ihrer Datenverarbeitung – so der Schutzzweck des § 303b StGB – abzustellen. Schon das Interesse der rechtmäßigen Nutzer von Computern, Laptops und Smartphones an dem ausschließlichen Gebrauchsrecht ihrer Geräte, unabhängig davon, ob ihre Daten beeinträchtigt werden oder sich Störungen im Funktionieren der Geräte zeigen, ist schützenswert. Wie der § 248b StGB zeigt, ist es der Systematik des Strafgesetzbuches nicht fremd, auch das schlichte Gebrauchsrecht an Sachen einem strafrechtlichen Schutz zu unterstellen.

In diesem Zusammenhang kann ein wirksamer Rechtsgüterschutz nicht davon abhängen, dass die Grundrechtsträger gehalten sind, für den Schutz ihrer IT-Systeme selbst zu sorgen. Wie das Bundesverfassungsgericht dargelegt hat, ist dies heutzutage bereits technisch kaum möglich (vgl. BVerfG, a. a. O.).

Ziel des Gesetzentwurfes soll es vor diesem Hintergrund sein, Artikel 2 des Budapester Übereinkommens über Computerkriminalität vom 23. November 2001 (BGBl. 2008 II S. 1242, „Convention on Cybercrime“) vollständig umzusetzen.

Dieser lautet:

„Artikel 2 – Rechtswidriger Zugang

Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um den unbefugten Zugang zu einem Computersystem als Ganzem oder zu einem Teil davon, wenn vorsätzlich begangen, nach ihrem innerstaatlichen Recht als Straftat zu umschreiben.

Eine Vertragspartei kann als Voraussetzung vorsehen, dass die Straftat unter Verletzung von Sicherheitsmaßnahmen, in der Absicht, Computerdaten zu erlangen, in anderer unredlicher Absicht oder in Zusammenhang mit einem Computersystem, das mit einem anderen Computersystem verbunden ist, begangen worden sein muss."

Diese Vorschrift ist durch § 202a StGB nur sehr eingeschränkt in das innerstaatliche Recht umgesetzt worden. Der damalige Bundesgesetzgeber hat von der Möglichkeit des Satzes 2 Gebrauch gemacht und als Voraussetzung für eine Strafbarkeit vorgesehen, dass die Straftat subjektiv auf Daten bezogen, objektiv unter Verletzung von Sicherheitsmaßnahmen begangen worden sein muss und nur solche Daten geschützt sind, die besonders gesichert sind. Der Gesetzgeber war damals der Auffassung, vor allem der letztgenannten Einschränkung auf solche Daten, die gegen unberechtigten Zugang besonders gesichert sind, komme eine besondere Bedeutung für die Eingrenzung des Tatbestandes zu, um Bagatellfälle auszufiltern (vgl. BT-Drucksache 16/3656 vom 30. November 2006).

Angesichts der heutigen arbeitsteiligen Vorgehensweise von Internetkriminellen und im Lichte der zitierten Entscheidung des BVerfG, wonach ein wirkungsvoller technischer Selbstschutz der Berechtigten kaum möglich ist, sind diese Einschränkungen indes überholt und stehen einer effektiven Strafverfolgung und dem Schutz der Bürger entgegen.

Hinzu kommt, dass angesichts der wachsenden Bedeutung der IT-Wirtschaft ein lückenhafter strafrechtlicher Schutz ein Nachteil für den Wirtschaftsstandort Deutschland gegenüber den Staaten darstellt, die Artikel 2 der Konvention vollständig und ohne Einschränkungen umgesetzt haben.

Es ist angezeigt, der ursprünglichen Intention der Konvention folgend, den unbefugten Zugang zu einem Computersystem („digitaler Hausfriedensbruch") und die dadurch eröffnete bloße Möglichkeit jedweden Datenzugriffs als Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme unter Strafe zu stellen. Dem berechtigten Anliegen, Bagatellfälle auszuscheiden, wird durch die Bagatellklausel und über die Ausgestaltung der Absätze 1 und 2 als Privatklagedelikt hinreichend Rechnung getragen.

Eine jüngst ergangene Entscheidung des BGH (vgl. Beschluss vom 21. Juli 2015, 1 StR 16/15) belegt eindrucksvoll die Lückenhaftigkeit des derzeitigen Rechtsgüterschutzes und das Leerlaufen von § 202a StGB selbst in gravierenden Fällen. Nach den Feststellungen des Landgerichts hatten die Angeklagten ein großes Botnetz aufgebaut und betrieben, das unter anderem der Erzeugung von Bitcoins, einer elektronischen Werteinheit, diente. Dazu nutzten die Angeklagten die Rechenleistung der von ihnen infiltrierten Opfersysteme aus. Das Gericht hatte in der Hauptverhandlung einen Sachverständigen des BKA zu den IT-technischen Fragen gehört und auf Grundlage seines Gutachtens, das auch schriftlich vorlag, die Funktionsweise der Schadsoftware in groben Zügen beschrieben. Der BGH hob die Verurteilungen mit folgender Begründung auf:

„(…) Die Verurteilung wegen Ausspähens von Daten in Tateinheit mit Datenveränderung (…) hält rechtlicher Nachprüfung nicht stand; der Schuldspruch wird von den getroffenen Feststellungen nicht getragen. Die Feststellungen sind teilweise lückenhaft und weisen zudem einen inneren, auch durch den Gesamtzusammenhang der Urteilsgründe nicht auflösbaren Widerspruch auf. Sie belegen nicht hinreichend, dass der Angeklagte jeweils eine Zugangssicherung überwunden hat, die für die Erfüllung des Straftatbestands des § 202a Abs. 1 StGB erforderlich ist. Denn der Schutzbereich dieser Strafvorschrift erstreckt sich nur auf Daten, die gegen unberechtigten Zugang besonders gesichert sind. Dies sind nur solche, bei denen der Verfügungsberechtigte durch seine Sicherung sein Interesse an der Geheimhaltung der Daten dokumentiert hat (vgl. BGH, Beschluss vom 6. Juli 2010 – 4 StR 555/09, NStZ 2011, 154). Die Zugangssicherung im Sinne von § 202a Abs. 1 StGB muss darauf angelegt sein, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren (vgl. BGH, Beschluss vom 6. Juli 2010 – 4 StR 555/09, NStZ 2011, 154; LK-StGB/Hilgendorf, StGB, § 202a Rn. 30; MüKo-StGB/Graf, StGB, § 202a Rn. 35; Rübenstahl/Debus, NZWiSt 2012, 129, 131). Darunter fallen insbesondere Schutzprogramme, welche geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte (vgl. BT-Drucks. 16/3656 S. 10).

Schließlich muss der Zugangsschutz auch gerade im Zeitpunkt der Tathandlung bestehen (vgl. MüKo-StGB/Graf, StGB, § 202a Rn. 20). Ob diese Voraussetzungen in den der Verurteilung zugrunde liegenden Fällen gegeben sind, vermag der Senat anhand der unvollständigen Feststellungen im Urteil nicht abschließend zu beurteilen. Zugleich kann nicht ausgeschlossen werden, dass das Landgericht der vorgenommenen Rechtsanwendung, die nicht näher erläutert wird (UA S. 13), ein fehlerhaftes Verständnis zugrunde gelegt hat. Es fehlt in den Urteilsgründen eine hinreichend genaue Darstellung der Wirkweise der von dem Angeklagten bereitgestellten Schadsoftware, welche die Benennung der im konkreten Einzelfall umgangenen Zugangssicherung erfasst. Der pauschale Verweis auf deren Bestehen reicht dafür ohne nähere Darlegung nicht aus, denn eine revisionsgerichtliche Kontrolle der eingangs genannten Voraussetzungen ist nur auf der Grundlage einer ausreichend deskriptiven Darlegung der konkreten tatsächlichen und technischen Umstände möglich. Die insoweit bestehende Lücke lässt sich durch die Feststellungen auch in ihrer Gesamtheit nicht schließen. Hinzu kommt, dass das Landgericht zwischen den Begrifflichkeiten der Firewall und des Virenschutzprogrammes nicht erkennbar differenziert hat, wodurch unklar bleibt, ob es die technischen Voraussetzungen der Zugangssicherung in tatsächlicher Hinsicht zutreffend bewertet hat. Während es zunächst nämlich darauf abstellt, der Trojaner sei so konzipiert gewesen, die vorinstallierte Firewall bestimmter Betriebssysteme zu umgehen (UA S. 3), findet sich im Widerspruch dazu an späterer Stelle der Urteilsgründe die Feststellung und Wertung, die vom Angeklagten bereitgestellte Schadsoftware sei durch die Virenprogramme der 327.379 Nutzer nicht erkannt worden (UA S. 4). Unter Zugrundelegung der zu der Schadsoftware zuletzt getroffenen Feststellungen käme eine Firewall als tatbestandsmäßige Schutzvorrichtung bereits dem Grunde nach nicht in Betracht. (…) Die dargelegten Rechtsfehler führen insgesamt zur Aufhebung des Urteils. Aufgrund desaufgezeigten Widerspruches und um dem neuen Tatrichter zu ermöglichen, umfassend stimmige eigene Feststellungen treffen zu können, waren auch die Feststellungen aufzuheben (§ 353 Abs. 2 StPO). Das neue Tatgericht wird Gelegenheit haben, sich mit den Handlungsabläufen in technischer und zeitlicher Hinsicht umfassender als bislang auseinanderzusetzen. Erst die hinreichend genaue Feststellung der technischen Gegebenheiten ermöglicht die strafrechtliche Bewertung der in Frage kommenden als solche bereits zutreffend erkannten Straftatbestände.“

Die Entscheidung verdeutlicht, dass die §§ 202a, 303a, 303b StGB in ihrer jetzigen Fassung bereits im Tatbestand untauglich sind, die heutigen Erscheinungsformen der Botnetzkriminalität wirkungsvoll zu bekämpfen. Die Anforderungen, die die Normen an die Strafjustiz stellen, sind für das Tatgericht kaum zu erfüllen. Dieses ist nach derzeitiger Rechtslage gehalten, nicht nur die Wirkungsweise der Zugangssicherung der Geschädigten im Einzelnen zumindest exemplarisch darzulegen, sondern auch die Veränderungen, die die Schadsoftware auf dem Opfersystem vorgenommen hat. Dies setzt voraus, dass solche Feststellungen überhaupt möglich sind. Verwenden die Täter jedoch eine Schadsoftware, die sich nach ihrem Einsatz selbsttätig löscht, fehlt es an dieser Möglichkeit.

Die Notwendigkeit für das Tatgericht, im Urteil zumindest exemplarisch detailliert darzulegen, welche technische Funktionsweise die Zugangssicherung der Opfersysteme in tatsächlicher Hinsicht jeweils hatte, bringt für die Besitzer der infiltrierten IT-Systeme erhebliche Belastungen mit sich. Die informationstechnische Funktionsweise der Zugangssicherung kann durch Zeugenbeweis der Berechtigten kaum in die Hauptverhandlung eingeführt werden, da die meisten Opfer Laien sind und häufig selbst nicht wissen, ob und wie ihr System zum Tatzeitpunkt in technischer Hinsicht geschützt war. Dies gilt besonders bei infiltrierten Mobiltelefonen.

Das wiederum bedeutet, dass zukünftig die Opfersysteme im Ermittlungsverfahren durch Sachverständige IT-forensisch zu untersuchen sind, um es dem Gericht später zu ermöglichen, in den Feststellungen deskriptiv die konkreten tatsächlichen und technischen Umstände des Zugangsschutzes darzulegen. Den Opfern der Infiltration entstehen neben dem Verlust von Daten und ihrer Privatheit aufgrund des Täterhandelns zusätzliche zeitliche Einbußen und Unannehmlichkeiten, weil sie den Sachverständigen der Staatsanwaltschaft (i. d. R. besonders ausgebildete Polizeibeamte) eine Datenspiegelung ermöglichen müssen. Eine derartige Spiegelung des IT-Systems bedeutet zwingend, dass höchstpersönliche Daten, auch aus dem Kernbereich, der Opfer ausgehändigt werden müssen. Auch wenn dies keine datenschutzrechtlichen Bedenken in sich birgt, da es sich um einen staatlichen Zugriff handelt, dürfte es aus Opfersicht gleichwohl zu einem Gefühl des Überwachtseins führen.

Unter der Geltung des neuen § 202e StGB hingegen stellen sich keine derartigen Probleme mehr. Die Tatsache des unbefugten Benutzens der Opfersysteme wird sich regelmäßig durch die Auswertung der Täterinfrastruktur und unter Einschaltung der Internetzugangsprovider anhand der IP-Adressen der Bots nachweisen lassen. Auf technische Zufälligkeiten kommt es nicht mehr an. Eine detaillierte Darstellung der technischen Einzelheiten der Infiltration im Ermittlungsverfahren, in der Anklageschrift und im Urteil ist nicht mehr notwendig. Dies führt zu

einer erheblichen Verfahrensbeschleunigung und zu einer Verkürzung der Auswertezeiten, ohne zu Lasten der Rechtssicherheit zu gehen.

Soweit die EU-Richtlinie 2013/40/EU vom 12. August 2013 über Angriffe auf Informationssysteme die von Botnetzen ausgehenden Gefahren thematisiert, dürfte formal kein Umsetzungsbedarf bestehen, da das Strafgesetzbuch, wie dargelegt, entsprechende Tatbestände enthält. Allerdings greifen diese Normen nicht lückenlos, um die in der Richtlinie beschriebene Bedrohung wirksam zu bekämpfen:

„(…) Es besteht eine Tendenz zu immer gefährlicheren und häufigeren Großangriffen auf Informationssysteme, die für den Mitgliedstaat oder für bestimmte Funktionen im öffentlichen oder privaten Sektor oft unverzichtbar sein können. Diese Tendenz geht einher mit der Entwicklung immer ausgefeilterer Methoden, wie etwa der Schaffung und Verwendung von sogenannten Botnetzen, bei denen die kriminelle Handlung in verschiedenen Stufen erfolgt, wobei jede Stufe für sich eine ernsthafte Gefahr für die öffentlichen Interessen darstellen könnte. Diese Richtlinie zielt unter anderem darauf ab, Strafen hinsichtlich der Schaffung der Botnetze einzuführen, nämlich für die Einrichtung einer ferngesteuerten Kontrolle über eine bedeutende Anzahl von Computern, indem diese durch gezielte Cyberangriffe mit Schadsoftware infiziert werden. Sobald es eingerichtet ist, kann das infizierte Netz von Computern, die das Botnetz bilden, ohne Wissen der Computerbenutzer aktiviert werden, um einen breit angelegten Cyberangriff zu starten, der in der Regel erheblichen Schaden anrichten kann (…)“

Präzise Fallzahlen in diesem Kriminalitätsbereich liegen nicht vor. Es ist von einem großen Dunkelfeld auszugehen, da die Geschädigten in aller Regel nicht wissen, dass ihre Rechner infiziert und ferngesteuert werden. Nur dann, wenn es zu einem missbräuchlichen Einsatz von ausgespähten Daten kommt, erfolgt unter Umständen eine Mitteilung an die Strafverfolgungsbehörden.

Die Erkenntnisse der nationalen und internationalen Strafverfolgungsorgane und Cybersicherheitszentren sowie diejenigen von IT-Wissenschaftlern belegen aber, dass die Fallzahlen und die daraus resultierenden Schäden deutlich steigen. In der ersten Jahreshälfte 2015 wurden von Sicherheitsforschern täglich bis zu 60 000 Infektionen deutscher Systeme registriert[10)]. Die polizeiliche Kriminalstatistik verzeichnet seit Jahren steigende Fallzahlen im Bereich der Delikte gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme und Daten.

Eine Momentaufnahme der Dimension des Problems gibt das Auffinden der 14 Millionen Opferdatensätze im Jahre 2014.

Weitere verlässliche Angaben über die Anzahl der infiltrierten Opfersysteme lassen sich aus der Analyse großer Botnetze gewinnen.

Bereits im Jahr 2011 wurde der jährliche, weltweit von für Botnetze verantwortlicher Schadsoftware verursachte Schaden in einer Studie, die das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) im Auftrag der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) erstellt hat, auf rund zehn Milliarden US Dollar geschätzt.

Den Medien sind für Deutschland Schadenssummen von 3,4 Milliarden Euro (DIW für 2014), über 54 Milliarden (Wirtschaftsberatungsgesellschaft KPMG für 2013/2014) bis hin zu 102 Milliarden Euro (Bitkom für 2013/2014) zu entnehmen. Aus Kreisen der Telekommunikationsprovider wird die Bandbreitennutzung des Internets durch Bot-Netze mit 80 Prozent beziffert. Auch hier dürfte von sehr hohen Schadenssummen auszugehen sein.

Laut Angaben eines US-amerikanischen IT-Sicherheitsdienstleisters aus dem Jahr 2013 habe das Botnetz „Chameleon“ ab 2012 beispielsweise einen Schaden von rund sechs Millionen USD im Monat für die Werbebranche verursacht. Über dieses Botnetz verbreitete Schadsoftware habe automatisiert Klicks auf Werbebanner simuliert, wobei für jeden Klick eine entsprechende Vergütung für den Internetdienstleister festgelegt war. Von 14 Milliarden Klicks auf ausgewählten Webseiten seien neun Milliarden auf dieses Bot-Netz zurückzuführen.

Allein der Schaden, der für Internet-Werbetreibende durch das ZeroAccess-Bot-Netz verursacht worden sein soll, wurde Ende 2013 auf rund 2,7 Millionen US-Dollar monatlich beziffert.

In den Jahren 2010 bis 2013 ermittelte die hessische Zentralstelle zur Bekämpfung der Internetkriminalität gemeinsam mit dem BKA in einem bundesweiten Verfahrenskomplex wegen einer Vielzahl von Erpressungen von Online-Shops mittels DDos-Attacken. Es konnten nach intensiven Ermittlungen fünf Beschuldigte identifiziert

---

[10)] Vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2015, S. 30

und vor Gericht gestellt werden, die in unterschiedlicher Zusammensetzung für die Erpressungen verantwortlich waren. Insgesamt konnten 40 Fälle aufgeklärt werden, in denen Betreiber von Webshops mit DDoS-Attacken bedroht oder tatsächlich angegriffen wurden. Die von den geschädigten Unternehmen auf die DDoS-Angriffe zurückzuführenden, geschätzten Umsatzeinbußen beliefen sich zusammen auf Beträge im mittleren sechsstelligen Bereich. Ein Unternehmen aus Hessen erlitt ein Schaden in Höhe von ca. 65 000 Euro.

Das Bundesamt für die Sicherheit in der Informationstechnologie geht in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2015“ davon aus, dass die Bedrohungslage durch Botnetze im Vergleich zum Vorjahr weiterhin kritisch und tendenziell steigend ist.

Eine Veränderung oder Anpassung der Regelungen der §§ 202a, 303a, 303b StGB ist zur Lösung des Problems nicht geeignet, da diese Normen andere Rechtsgüter als die Vertraulichkeit, die Integrität und das ausschließliche Gebrauchsrecht an informationstechnischen Systemen schützen. Botnetzaktivitäten wie das Versenden von Spam oder das Generieren von Bitcoins greifen nicht zwingend in das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit von Daten oder in das Interesse der Betreiber und Nutzer am störungsfreien Funktionieren ihrer Datenverarbeitung ein. Auch werden Daten nicht zwingend ausgespäht. Dies rechtfertigt es, die genannten Regelungen des StGB unverändert neben der neuen Strafnorm des § 202e StGB bestehen zu lassen.

II. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes.

III. Auswirkungen

Durch die Einführung eines neuen Straftatbestands kann mehr Aufwand bei den Strafverfolgungsbehörden entstehen, dessen Umfang im gegenwärtigen Zeitpunkt nicht hinreichend genau abschätzbar ist. Im Übrigen wird das Vorhaben Bund, Länder, Gemeinden, die Wirtschaft und die Bürger nicht mit Mehrkosten belasten. Da sich der Gesetzentwurf auf Änderungen und Ergänzungen von Strafvorschriften beschränkt, sind Auswirkungen auf das Preisniveau, insbesondere auf das Verbraucherpreisniveau, die Umwelt oder Auswirkungen von gleichstellungspolitischer Bedeutung nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Strafgesetzbuches)

Zu Nummer 1 (Inhaltsübersicht zu § 202e StGB)

Es handelt sich um eine redaktionelle Folgeänderung im Hinblick auf die Einfügung des § 202e StGB-E (Nummer 2).

Zu Nummer 2 (§ 202e – neu – StGB)

Die vorgeschlagene Regelung soll als neuer § 202e StGB in den Fünfzehnten Abschnitt (Verletzung des persönlichen Lebens- und Geheimbereichs) des Besonderen Teils des Strafgesetzbuchs eingefügt werden. Für eine systematische Regelung an dieser Stelle spricht, dass das geschützte Rechtsgut der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dem persönlichen Lebens- und Geheimbereich zuzuordnen ist.

Zu Absatz 1

Das Merkmal der Unbefugtheit als allgemeines Rechtfertigungselement entspricht dem in § 201 verwendeten Begriff. Es stellt klar, dass eine Strafbarkeit bei wirksamer ausdrücklicher oder konkludenter Einwilligung ausgeschlossen ist. Dadurch ist es z. B. nicht strafbar, wenn Betreiber von Internetseiten Cookies[11)] verwenden und darauf, wie es datenschutzrechtlich geboten und üblich ist, hinweisen. Auch das Aufspielen von Softwareupdates

---

[11)] Ein Cookie (engl. "Keks") ist eine Textinformation, die eine besuchte Website (hier "Server") über den Browser im Rechner des Betrachters ("Client") platziert. Der Client sendet die Cookie-Information bei späteren, neuen Besuchen dieser Seite mit jeder Anforderung wieder an den Server.

o. ä. ist hierdurch von Strafbarkeit ausgenommen, ebenso wie z. B. das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens, soweit der „Hacker“ vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde. Auch sonst sozialadäquate Handlungen sind nicht „unbefugt“ im Sinne von § 202e StGB-E (zur Sozialadäquanz bei anderen Delikten im 15. Abschnitt vgl. Fischer, StGB, 63. Auflage, Erläuterungen zu § 201).

Durchaus erfasst sind hingegen beispielsweise Applikationen (Apps) für Endgeräte, die einen größeren Funktionsumfang haben als in der jeweiligen Beschreibung oder Datenschutzerklärung angegeben, bei deren Installation die Nutzer mithin bewusst über die eingeräumten Zugriffsrechte getäuscht werden.

§ 202e StGB-E hat erfüllt insoweit auch einen bedeutenden Zweck im Zivilrecht, indem die Funktion eines Schutzgesetzes im Sinne von § 823 Absatz 2 BGB eingenommen und damit auch zivilrechtlich ein besserer Verbraucherschutz erreicht wird.

Auf die Beschränkung des Tatbestandes auf „fremde“ informationstechnische Systeme wurde bewusst verzichtet, um auch Fälle zu erfassen, in denen z. B. ein Arbeitnehmer ein mobiles IT-System des Arbeitgebers zur alleinigen Benutzung erhält und der Arbeitgeber dieses heimlich infiltriert hat, um unbefugt in den persönlichen Lebens- und Geheimbereich des Arbeitnehmers einzudringen. Auch sollen z. B. Hotelgäste bei der Benutzung für sie fremder IT-Systeme vor Infiltration der von ihnen verarbeiteten Informationen durch den Eigentümer des Systems geschützt werden.

Die Anwendungspraxis des seit 1953 geltenden § 248b StGB zeigt, dass grundsätzliche Probleme durch die Einführung eines weiteren Falles des strafbewehrten Verbots der unbefugten Benutzung von Sachen in das Strafgesetzbuch nicht zu erwarten sind.

Das informationstechnische System ist in Absatz 6 legaldefiniert. Es sollen nur solche Geräte, Anlagen etc. geschützt sein, die objektiv eine besondere Bedeutung für den Berechtigten haben oder deren Fremdnutzung besonders gefährdungsintensiv ist und die damit in herausgehobener Weise schutzwürdig sind. Damit sind z. B. nicht vernetzte elektronische Unterhaltungsgeräte, Spielzeug oder Taschenrechner aus dem Tatbestand ausgeklammert.

Zugleich stellt die Bagatellklausel des Absatzes 1 Satz 2 eine mit derjenigen des § 201 StGB inhaltsgleiche Tatbestandseinschränkung dar. Nach dieser ist die Tathandlung nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Ob es sich dabei um materielle oder ideelle, private oder öffentliche Interessen handelt, ist gleichgültig, sofern sie nur vom Recht als schutzwürdig anerkannt sind oder diesem jedenfalls nicht zuwiderlaufen. Dass der Betroffene tatsächlich in seinen Interessen beeinträchtigt wird, ist nicht erforderlich; vielmehr genügt es schon, dass die Tat dazu geeignet ist.

Durchgreifende verfassungsrechtliche Bedenken gegen die Bagatellklausel unter dem Aspekt des Bestimmtheitsgrundsatzes (Artikel 103 Absatz 2 des Grundgesetzes) bestehen nicht. Sie ist in § 201 StGB in derselben Formulierung wie in § 202e StGB-E unverändert in Kraft seit dem 26. August 1990. Obwohl das BVerfG sich bereits im Jahr 2010 mit § 201 StGB befasst hat, wurde die Bagatellklausel nicht beanstandet[12)].

Ein Datenverarbeitungsvorgang (DV-Vorgang) ist ein Arbeitsablauf, der durch eine elektronische Verarbeitung zu einem konkreten Ergebnis führt [13)]. Auf Grund bestimmter Eingabedaten (Input) muss mit dem im Computer gespeicherten Programm – ggf. ergänzt durch weitere Eingaben zur Steuerung – ein Arbeitsergebnis erzielt und ausgegeben werden (Output).

Da auch elektronisch fernzusteuernde Anlagen und Einrichtungen geschützt werden sollen, auf denen selbst keine DV-Vorgänge im vorbeschriebenen juristischen Sinne ablaufen (z. B. ein fernwartbares Schleusentor, das durch einen schlichten Öffnen/Schließen-Befehl reagiert, ohne dass dazu ein Computerprogramm abläuft), wurde zusätzlich der Begriff des informationstechnischen Ablaufs aufgenommen. Nach der Legaldefinition des § 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) ist damit jede Verarbeitung oder Übertragung von Informationen durch technische Mittel gemeint. Dies ist weitergehend als der Begriff des DV-Vorgangs. Es soll sichergestellt werden, dass der strafrechtliche Schutz von Automatisierungs-, Prozesssteuerungs- und Prozessleitsystemen (Industrial Control Systems, ICS) gewährleistet wird, um den Rechtsrahmen für Industrie 4.0 zu verbessern.

---

12) Vgl. BVerfG NJW 2011, 1863

13) Vgl. Lenckner/Winkelbauer CR 1986, 654, 658 f; Fischer, StGB, § 263a Rn 3.

Aus diesem Grunde erstreckt sich der Schutzbereich von § 202e StGB-E nicht lediglich auf Datenverarbeitungsanlagen oder Datenverarbeitungen wie §§ 303a StGB oder 303b StGB, sondern geht darüber hinaus.

„Zugang“ ist die Möglichkeit, ohne weitere Zwischenschritte einen IT-Vorgang auszulösen oder zu beeinflussen. Gemeint ist damit sowohl der physische, unmittelbare Zugriff als auch derjenige über Datenleitungen. Der Zugang ist erlangt, wenn das System infiltriert, also eine etwaige Sperre überwunden und der Täter in der Lage ist, Eingaben unmittelbar vorzunehmen.

Es wird nicht verkannt, dass die Regelung des Absatzes 1 einen weiten Anwendungsbereich hat. Die Bagatellklausel sorgt jedoch dafür, dass nicht strafwürdige Fälle von dem Tatbestand zuverlässig ausgeschlossen werden. Ferner sorgt die Begrenzung auf bestimmte IT-Systeme in Absatz 6 dafür, dass nicht schutzwürdige Systeme wie z. B. eine Modelleisenbahn von der Norm nicht erfasst werden.

Die Anwendungspraxis des geltenden Rechts hat gezeigt, dass jede weitergehende Einschränkung des Tatbestandes dazu führt, dass ein hinreichender strafrechtlicher Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht erreicht werden kann. Die mangelnde Effektivität der geltenden Normen lässt sich durch die trotz der hohen Zahl betroffener Opfer auffällig niedrigen Verurteilungszahlen [14)] empirisch belegen.

Die Verhängung von Strafe als ultima ratio des Staates zur Verhütung von Sozialschäden ist dann nicht am Platze, wenn das Opfer keinen Schutz verdient und keines Schutzes bedarf, weil es von ohne weiteres verfügbaren Selbstschutzmöglichkeiten ohne triftigen Grund keinen Gebrauch gemacht hat. Genau diese Selbstschutzmöglichkeit besteht heutzutage angesichts der Komplexität von IT-Systemen einerseits und derjenigen von Schadsoftware andererseits eben nicht mehr.[15)]

Zu Absatz 2

Absatz 2 enthält eine höhere Strafdrohung für gefährdungsintensivere Begehungsweisen.

Zu Absatz 3

Die Strafzumessungsvorschriften des Absatzes 3 finden sich in ähnlicher Weise z. B. in § 263 Absatz 3 StGB.

Nummer 3 ist eine deliktsspezifische Regelung, die dem Umstand Rechnung trägt, dass Industrie- oder ähnlich bedeutsame Anlagen heutzutage vielfach über Internet angreifbar sind.

Zu Absatz 4

Absatz 4 enthält eine Qualifikation, da die auch im BSI-Gesetz legaldefinierten Kritischen Infrastrukturen eines besonders intensiven strafrechtlichen Schutzes bedürfen.

Zu Absatz 5

Die Versuchsstrafbarkeit ist notwendig, um z. B. beim Einsatz nicht offen ermittelnder Polizeibeamter oder verdeckter Ermittler dennoch zu einer Strafbarkeit des Täters zu gelangen. Der Einsatz von derartigen Ermittlungsmethoden ist bei Internetermittlungen von hoher praktischer Relevanz. In solchen Fällen wird jedoch häufig ein untauglicher Versuch gegeben sein. Die Legitimationsgrundlage für die Strafbarkeit des untauglichen Versuchs liegt in der durch das Ansetzen zur Tat, also einer objektiven Betätigung, zum Ausdruck kommenden Missachtung des Normbefehls als Rechtsfriedensstörung.

Zu Absatz 6

Wie bereits oben dargelegt, sollen bestimmte, nicht schutzwürdige IT-Systeme vom Tatbestand ausgenommen werden. Die Eignung zur Verarbeitung personenbezogener Daten und die Nutzung als Steuerungskomponente für bestimmte Anwendungen begründen die Schutzwürdigkeit des Systems.

Der Begriff der „Kritischen Infrastruktur“ ist mit demjenigen in § 2 Absatz 10 BSIG identisch. Eine kritische Infrastruktur im Sinne des § 202e StGB-E kann daher nur eine solche sein, die die Kriterien der Verordnung zur

---

14) Vgl. Strafverfolgungsstatistik 2013 (Statistisches Bundesamt, Fachserie 10, Reihe 3): 30 Verurteilungen wegen § 202a StGB, 32 wegen § 303a StGB und 26 wegen § 303b StGB

15) Vgl. BVerfG a.a.O.

Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz vom 22. April 2016 (BGBl. I 2016, 958) erfüllt, also z. B. eine Anlage, von deren Versorgungsleistung jeweils 500 000 oder mehr Bürger abhängig sind.

Zu Absatz 7

Durch diese Regelung soll die Strafverfolgung bei Fällen im Nähebereich begrenzt werden, um bestimmte persönliche Beziehungen durch Eingreifen von Amts wegen nicht zu stören.

Zu Nummer 3 (§ 205 Absatz 1 Satz 2 StGB)

Angesichts des im Einzelfall unter Umständen geringeren Unwertgehalts von Taten nach den Absätzen 1 und 2 ist § 202e StGB-E in den Kreis der relativen Antragsdelikte nach § 205 Absatz 1 Satz 2 StGB aufzunehmen. Ein Einschreiten von Amts wegen bei besonderem öffentlichen Interesse an der Strafverfolgung soll ermöglicht werden.

Zu Artikel 2 (§ 374 Absatz 1 Nummer 3a StPO)

Es handelt sich um eine Folgeänderung der Strafprozessordnung. Aufgrund seiner Nähe zu anderen in § 374 Absatz 1 StPO genannten Delikten, die dem Schutz höchstpersönlicher Rechtsgüter dienen, soll auch § 202e StGB-E in den Kreis der Privatklagedelikte aufgenommen werden. Wie die in § 374 Absatz 1 StPO genannten Vergehen kann eine unbefugte Benutzung eines IT-Systems, ein digitaler Hausfriedensbruch, in den Fällen der Absätze 1 und 2 die Allgemeinheit mitunter so wenig berühren, dass kein öffentliches Interesse an der Strafverfolgung besteht. In Durchbrechung des Offizialprinzips soll in einem solchen Fall ausnahmsweise der Verletzte bzw. dessen gesetzlicher Vertreter oder ein sonstiger Strafantragsberechtigter die Strafverfolgung als Privatkläger selbst betreiben dürfen.

Mit der Ausgestaltung der Absätze 1 und 2 als Privatklagedelikt soll der Notwendigkeit Rechnung getragen werden, einer Überlastung der Strafverfolgungsbehörden durch Bagatellfälle vorzubeugen.

Ein Wertungswiderspruch zu den erhöhten Mindeststrafen der Absätze 3 und 4 ist hierin nicht zu sehen, weil der Unwertgehalt der Grundkonstellationen in den ersten beiden Absätzen sich erheblich vom Unwertgehalt der Qualifikation und besonders schweren Fälle unterscheidet.

Zu Artikel 3 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten. Das Gesetz soll am Tag nach der Verkündung in Kraft treten.

Anlage 2

Stellungnahme der Bundesregierung

Die Bundesregierung nimmt zu dem Gesetzentwurf des Bundesrates wie folgt Stellung:

Der Gesetzentwurf des Bundesrates sieht vor, einen neuen Straftatbestand der unbefugten Benutzung informationstechnischer Systeme mit einer Strafandrohung von Geldstrafe oder Freiheitsstrafe bis zu einem Jahr zu schaffen (§ 202e des Strafgesetzbuchs in der Entwurfsfassung [StGB-E]). Bestraft werden soll danach, wer unbefugt sich oder einem anderen Zugang zu einem informationstechnischen System verschafft, es in Gebrauch nimmt oder den Datenverarbeitungsvorgang oder informationstechnischen Ablauf des Systems beeinflusst oder in Gang setzt. Erfasst wäre davon beispielsweise die unerlaubte Nutzung eines Mobiltelefons. Die Tat soll strafbar sein, „wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen“ (§ 202e Absatz 1 Satz 2 StGB-E). Bei Handeln gegen Entgelt oder in Bereicherungsabsicht soll Geldstrafe oder Freiheitsstrafe bis zu fünf Jahren angedroht werden (§ 202e Absatz 2 StGB-E). Für besonders schwere Fälle ist eine Strafschärfung bis zu zehn Jahren Freiheitsstrafe vorgesehen (§ 202e Absatz 3 StGB-E). Handelt der Täter mit der Absicht, die Funktionsfähigkeit kritischer Infrastruktur zu beeinträchtigen oder deren Ausfall zu bewirken, soll dies als Verbrechen mit einer Freiheitsstrafe von mindestens einem Jahr geahndet werden können (§ 202e Absatz 4 StGB-E).

Der Bundesrat begründet seinen Gesetzentwurf vor allem damit, dass Täter vermehrt fremde informationstechnische Systeme infiltrierten, sie zu sogenannten Botnetzen zusammenschlössen und für kriminelle Zwecke einsetzten, ohne dass die rechtmäßigen Nutzer dies bemerkten und wirksam verhindern könnten. Die unter der Kontrolle der Täter stehenden Botnetze würden insbesondere für koordinierte Angriffe auf Websites und elektronische Infrastrukturen sowie für sonstige Internetstraftaten eingesetzt und erlaubten den Tätern anonym zu bleiben. Das geltende Strafrecht decke dies nicht ausreichend ab, da insbesondere das Ausspähen von Daten nach § 202a StGB nur strafbar ist, wenn der Täter eine Zugangssicherung überwindet, was bei Fällen der unbefugten Nutzung von informationstechnischen Systemen vielfach jedenfalls nicht nachweisbar sei.

Die Bundesregierung teilt die Auffassung des Bundesrates, dass Botnetz-Kriminalität auch mit den Mitteln des Strafrechts bekämpft werden muss. Allerdings bestehen nach Ansicht der Bundesregierung dabei jedenfalls keine gravierenden Strafbarkeitslücken. Nahezu sämtliche Aktivitäten beim Aufbau und Betrieb eines Botnetzes unterfallen bereits nach geltendem Recht Straftatbeständen des Strafgesetzbuches. Das Programmieren eines entsprechenden Schadprogramms, das dem Täter Zugang zu und Kontrolle über informationstechnische Systeme ermöglicht, ist als Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB) unter Strafe gestellt. Der Aufbau eines Botnetzes mit Hilfe von Schadprogrammen ist in aller Regel als Ausspähen von Daten (§ 202a StGB) strafbar. Soweit die Schadsoftware Daten verändert, liegt der Straftatbestand der Datenveränderung (§ 303a StGB) vor. Angriffe auf Informationssysteme mit Hilfe von ferngesteuerten Botnetzen (DDoS-Attacken) erfüllen den Tatbestand der Computersabotage (§ 303b Absatz 1 Nummer 2 StGB).

Die Strafbarkeit des Ausspähens von Daten (§ 202a StGB) setzt nach geltendem Recht voraus, dass die Daten gegen unberechtigten Zugang besonders gesichert sind und der Täter diese Zugangssicherung überwindet. Dies erscheint nach wie vor sachgerecht und vorzugswürdig gegenüber einer Strafbarkeit der (Mit-)Nutzung informationstechnischer Systeme, die der Berechtigte selbst ungeschützt gelassen hat. Eine derart weitgehende Strafbarkeit hätte auch in der „analogen Welt“ kein Vorbild. Nach dem Gesetzentwurf des Bundesrats wäre das unbefugte Einschalten des nicht durch ein Passwort gesicherten Mobiltelefons (eines anderen) eine Straftat, während das unbefugte Aufschlagen und Lesen eines fremden Notiz- oder Tagebuchs wie bisher straflos bleibt. Die vom Bundesrat angeführten Schwierigkeiten beim Nachweis der Zugangssicherung, die es im Einzelfall geben mag, können die Begründung der Strafwürdigkeit nicht ersetzen.

Die im Gesetzentwurf des Bundesrates vorgesehene Einschränkung des Tatbestands durch eine Bagatellklausel (§ 202e Absatz 1 Satz 2 StGB-E) lässt offen, wann eine Eignung zur Beeinträchtigung berechtigter Interessen gegeben sein soll, und dürfte zu erheblicher Rechtsunsicherheit führen, zumal der Gesetzentwurf nicht nur informationstechnische Systeme erfassen will, die zur Verarbeitung personenbezogener Daten geeignet oder bestimmt sind (§ 202d Absatz 6 Nummer 1 Buchstabe a StGB-E), sondern auch Systeme, die Teil bestimmter technischer

Einrichtungen und Anlagen sind (§ 202d Absatz 6 Nummer 1 Buchstabe b StGB-E), und damit zwei ganz unterschiedliche Schutzrichtungen verfolgt. Der Hinweis auf die gleichlautende Bagatellklausel bei der Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) vermag nicht vollständig zu überzeugen, da es dort um eine enger umschriebene Tathandlung geht (öffentliche Mitteilung heimlicher Aufnahmen) und im Zusammenhang mit dem Rechtsgut der Privatsphäre eine Abgrenzung leichter möglich ist. Berechtigte Interessen im Sinne des vorliegenden Gesetzentwurfs dürften in der Regel dann berührt sein, wenn mit der Tat Zugang zu geschützten Daten erlangt wird oder Daten verändert werden. In diesen Fällen ist aber bereits nach geltendem Recht eine Strafbarkeit gegeben (§§ 202a, 303a StGB).

Schließlich bestehen Bedenken insbesondere hinsichtlich der hohen Strafandrohung von mindestens einem Jahr bis zu zehn Jahren Freiheitsstrafe für den Fall, dass der Täter in der Absicht handelt, den Ausfall oder eine Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken (§ 202e Absatz 4 StGB-E), da die Einstufung als Verbrechen an einem subjektiven Element festgemacht wird, ohne dass es objektiv zu einer Gefährdung oder Beeinträchtigung einer kritischen Infrastruktur kommen muss.

Trotz der Bedenken anerkennt die Bundesregierung grundsätzlich das Ziel des Gesetzentwurfs des Bundesrates und wird im weiteren Verfahren prüfen, ob und inwieweit Strafbarkeitslücken ein gesetzgeberisches Handeln erforderlich machen und gegebenenfalls einen eigenen Gesetzentwurf vorlegen.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333